

MEDIDAS BÁSICAS DE SEGURANÇA DA INFORMAÇÃO APLICADAS EM UM CFC (CENTRO DE FORMAÇÃO DE CONDUTORES)

Elaborador:	Eduardo Barbosa Sirino
Orientador:	Prof. Edson Roberto Gaseta
Aprovadores:	Prof. Márcio Roberto Baldo Taglietta e Prof. Henri Alves de Godoy

**FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte**

S634m SIRINO, Eduardo Barbosa

Medidas básicas de segurança da informação aplicadas em um CFC (Centro de Formação de Condutores). / Eduardo Barbosa Sirino. – Americana, 2018.

37f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Edson Roberto Gasetta

1 Segurança em sistemas de informação I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU:681.518.5

Faculdade de Tecnologia de Americana

Eduardo Barbosa Sirino

**MEDIDAS BÁSICAS DE SEGURANÇA DA INFORMAÇÃO
APLICADAS EM UM CFC (CENTRO DE FORMAÇÃO DE
CONDUTORES)**

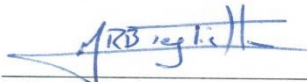
Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.
Área de concentração: Segurança da Informação

Americana, 07 de dezembro de 2018.

Banca Examinadora:



Edson Roberto Gaseta
Especialista
FATEC Americana



Márcio Roberto Baldo Taglietta
Especialista
FATEC Americana



Henri Alves de Godoy
Mestre
FATEC Americana

SUMÁRIO

1	OBJETIVO DESTE DOCUMENTO	1
2	VISÃO EMPRESARIAL SOBRE A SEGURANÇA DA INFORMAÇÃO	3
3	AMBIENTE DE APLICAÇÃO DAS MELHORIAS	5
3.1	Ambiente antes das mudanças	12
3.2	Ambiente depois das mudanças	15
3.2.1	Active Directory	15
3.2.2	VPN	18
3.2.3	Inventário e Organização	24
3.2.4	<i>Backup</i>	29
4	RESULTADOS OBTIDOS	34
4.1	Interligação das unidades	34
4.2	Controle de Usuários	35
4.3	Organização do parque computacional	36
4.4	<i>Automatização do Backup</i>	37
5	CONCLUSÃO E CONSIDERAÇÃO FINAL	38

Lista de figuras

Figura 1 - Tripé da Segurança da Informação	3
Figura 2 - Organograma Organizacional.....	6
Figura 3 - Distribuição dos dispositivos de rede no térreo da matriz	9
Figura 4 - Distribuição dos dispositivos de rede na filial do centro.....	10
Figura 5- Distribuição dos dispositivos de rede na filial do Europa.	11
Figura 6- Distribuição dos dispositivos de rede na filial do Mollon.	11
Figura 7 - Exemplo conexão do usuário.....	12
Figura 8 - Assistente de criação de backup System CFC-B.....	14
Figura 9 - Exemplo organização por setores.....	16
Figura 10 - Políticas para os perfis de usuários.....	17
Figura 11 - Políticas para computadores	17
Figura 12 – Conexão VPN.....	19
Figura 13 - Exemplo do arquivo de configuração	20
Figura 14 - Arquivos de Configuração cliente	21
Figura 15 - Arquivo de configuração do cliente.....	22
Figura 16 – Tela abertura de chamados no modo usuário	26
Figura 17 – Foto real do antes e depois da organização dos cabos	28
Figura 18 – Propriedades das tarefas	30

Lista de tabelas

Tabela 1 - Programas padrão dos computadores	24
--	----

1 OBJETIVO DESTE DOCUMENTO

Este relatório técnico, consiste na aplicação de medidas básicas de segurança da informação dentro de uma pequena empresa. O objetivo é trazer um comparativo entre os cenários de antes e depois e, recomendações relacionadas ao que foi aplicado. Pode-se relacionar as medidas de segurança, como a adoção de políticas de TI (Tecnologia da Informação), organização de fluxo de dados, organização do parque computacional, automatização de processos e proteção a informação.

A digitalização nos processos de trabalho se tornou muito comum nos mais diversos ambientes organizacionais, até mesmo nos mais simples deles. A tecnologia torna os processos mais econômicos, confiáveis e gerenciáveis, sendo um grande atrativo aos empresários. As empresas que estão se adequando a esse novo mundo estão economizando muito dinheiro e recursos, que podem ser revertidos para futuros investimentos e/ou na redução dos custos, garantindo maior competitividade e aumento da sua demanda.

As vantagens trazidas pela digitalização, também trazem consigo a necessidade do gerenciamento de todo tráfego de dados e de segurança. Nessa linha entram os profissionais de TI, que propõem e adequam soluções para cada ambiente corporativo. São esses profissionais responsáveis por entender a necessidade de cada cliente e aplicar soluções que viabilizam a forma de trabalho de cada um.

Para controlar todas as informações digitais geradas pelas empresas, os profissionais de TI utilizam várias ferramentas de auxílio e sistemas de informação, que centralizam e tornam compreensíveis os dados gerados. Os profissionais devem ser capacitados para controlar cada nível de acesso de acordo com a hierarquia de cada empresa, além de serem responsáveis por resguardarem os dados e os tornarem disponíveis pelos seus respectivos donos.

Para o sucesso da execução, foi necessário a aprovação devida da propriedade privada, aqui abordada. Essa propriedade denominada CFC Brasil, atua na área de prestação de serviços para formação de condutores das categorias “A”,

“B”, “C”, “D” e “E”, (Moto, Carro, Carga simples, Passageiros e Cargas especiais), eles contam com estruturas de atendimento em quatro localidades na cidade Santa Bárbara D’Oeste - SP, sendo: A matriz localizada no bairro Jd. Pérola, que é responsável pela administração; A filial do Centro localizada no centro de Santa Barbara D’Oeste; A filial do Mollon localizada no bairro Mollon de Santa Barbara D’Oeste; E a filial do Europa, localizada no bairro Jd. Europa de Santa Barbara D’Oeste. Todos esses ambientes são informatizados e se comunicam entre si.

Na matriz concentra-se a: administração, diretoria e a TI. Todos os processos realizados pelas filiais são redirecionados e tratados pela matriz, que envia ao DETRAN (Departamento Estadual de Trânsito) as informações necessárias de cada unidade.

Baseando-se nessa estrutura de trabalho do CFC Brasil, o relatório abordará, com todos os detalhes, a implementação dos controles e medidas adotadas pelo profissional de TI, antecedido por conceitos relacionados à segurança da informação. Também será apresentado de forma detalhada o ambiente antes das implementações.

O final do desenvolvimento será destinado a comparação entre os dois ambientes descritos. Serão relacionados todos os ganhos obtidos, tudo o que foi possível ser realizado ou não, todos os investimentos necessários para execução e o custo benefício dessa implementação.

2 VISÃO EMPRESARIAL SOBRE A SEGURANÇA DA INFORMAÇÃO

Formada por um conjunto de características voltadas à proteção da informação, a segurança da informação conta como base a: confidencialidade, integridade e disponibilidade, cada uma dessas características tem um papel muito importante para que a segurança funcione de fato (SÊMOLA, 2003, p.45), conforme a Figura 1:

Figura 1 - Tripé da Segurança da Informação



Fonte: DEBSOLUTIONTI (2015).

Segundo o autor Sêmola, (2003) pg.45, essas características podem ser definidas da seguinte maneira:

Confidencialidade

Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas as pessoas para quem elas são destinadas.

Integridade

Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

Disponibilidade

Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Para Benetti (2015), o conceito mais interessante dos três pilares é a confidencialidade, talvez por ter a ver com sigilo e segredo, isso mexe com a curiosidade humana. No mundo corporativo, também é o aspecto mais estratégico, pois a confidencialidade da informação protege o capital intelectual e por consequência as vantagens competitivas da empresa.

Sêmola (2003), comenta também os conceitos de segurança da informação sobre outros dois aspectos muito importantes que derivam dos três pilares que são a: legalidade e autenticação. Esses dois elementos estão diretamente ligados ao funcionamento legal da instituição dentro da legislação vigente e da discriminação de ações em processos digitais que ocorrem também na instituição.

Sêmola (2003), completa dizendo que a segurança da informação passou a ser vista como um ativo nos negócios, ela se tornou algo indispensável no ambiente empresarial. As interconexões entre empresas, comércios e clientes finais estão se tornando mais comuns e estão trazendo consigo a necessidade de proteção dos dados trafegados.

A busca para adesão dos processos de trabalho com base nos pilares da segurança da informação é muito grande e necessária, não é um trabalho fácil nem rápido, é preciso muito empenho e tempo para adequação de todo ambiente. A preparação para as mudanças precisa ser gradual e constante para que não prejudique o objetivo do negócio. Seguindo esses princípios, esse relatório foi construído demonstrando o início dessa adesão.

3 AMBIENTE DE APLICAÇÃO DAS MELHORIAS

O ambiente tecnológico encontrado na empresa CFC Brasil antes das mudanças estava bem desatualizado, não continha muitos controles administrativos, o monitoramento e acompanhamento era bem esporádico e a preocupação com a segurança estava relacionada somente aos *backups*, mas de certa forma todo o sistema funcionava e atendia o propósito do negócio.

Segundo a empresa CFC Brasil (2015), a sua missão é ser e fazer a diferença no trânsito, tendo como diferencial a: prestação de serviços de qualidade, transparência e agilidade para que o futuro condutor obtenha a CNH (Carteira Nacional de Habilitação) da melhor forma possível.

Com o ambiente tecnológico desorganizado e sem regras, não seria possível colaborar com as missões e objetivos presados pelo CFC Brasil. Mudanças e melhorias dentro do possível foram implementadas para colaborar.

Havia incidência frequente de: perda de dados, vírus na rede, queda de internet, travamento em impressoras, equipamentos não identificados e desinformação sobre os procedimentos informáticos. A proposta aplicada que será descrita nesse capítulo, melhora cada um desses itens.

Afim de explicar a estrutura organizacional atual para o embasamento do leitor, será apresentado um pouco de como é constituída a empresa CFC Brasil. A hierarquia segue os padrões estabelecidos pelo SEBRAE (2018), que exige alguns cargos para seu funcionamento legal.

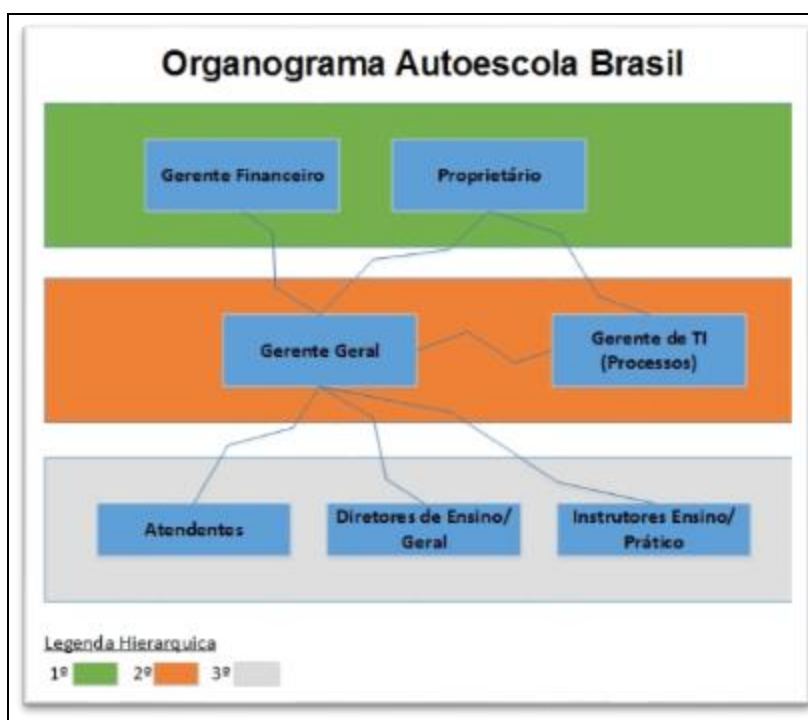
Somando todos os colaboradores do CFC Brasil, foram contabilizados cinquenta e quatro contribuintes, sendo eles:

- 30 Instrutores práticos
- 11 Atendentes / Auxiliares administrativos
- 1 Gerente Geral

- 1 Técnico de TI
- 1 Gerente financeiro
- 4 Diretores de ensino
- 1 Diretor Geral
- 4 Instrutores teóricos
- 1 Proprietário

Distribuídos em um organograma, pode se identificar a posição de cada colaborador, na Figura 2:

Figura 2 - Organograma Organizacional



Fonte: Próprio autor.

Como mencionado na introdução, a empresa CFC Brasil possui quatro unidades. Na Matriz do Jd. Pérola concentra-se: O atendimento e as vendas, a administração da empresa, o setor de Tecnologia da Informação e o CFC “A” (Centro de Formação de Condutores Teórico).

As outras filiais como Centro, Mollon e Europa são responsáveis somente pelas vendas e o atendimento ao público (pós-venda). A filial do Centro possui um único diferencial das demais, que é a possibilidade de realizar aulas de simulador no local.

Seguindo os requisitos mínimos de funcionamento descrito pelo Sebrae na aba “exigências legais e específicas” para um CFC, o CFC Brasil apresenta total conformidade com os requisitos de estrutura e informática (SEBRAE, 2007).

A comunicação realizada entre CFC x DETRAN é realizada através de um sistema online, chamado e-CNHsp. Esclarecido pela Prodesp (2010), “O e-CNHsp é o novo sistema utilizado pelo Detran.SP, operado online por internet, para a execução de serviços relacionados à habilitação de condutores”. Para o funcionamento adequado, o sistema e-CNHsp (2011), exige que os profissionais (diretores de ensino e instrutores) possuam as credencias sempre em dia e que os procedimentos de autenticação sejam realizados através do e-CPF, garantindo a veracidade das informações e responsabilidade dos profissionais.

Todos os procedimentos realizados no CFC referente ao processo de habilitação do aluno, são informados ao sistema e-CNHsp, para que ao final do processo seja possível a confecção da CNH.

A alimentação dos dados no sistema e-CNHsp é realizada pelos instrutores e diretores de ensino prático ou teórico. A alimentação baseia-se: na matrícula do aluno, vínculo do CFC e aluno, lançamento de aulas práticas e teóricas, marcação dos exames prático e teórico e nas emissões de certificados de conclusão e LADVs (Licença de Aprendizagem de Direção Veicular). Para que esses procedimentos sejam realizados é necessário que o CFC possua alguns dispositivos especiais, como os leitores de cartão inteligente, portas USB e leitores biométricos *Live Finger* (Dedo Vivo) homologados pelo DetranSP. (SÃO PAULO, 2016).

Além dos equipamentos físicos, o e-CNH necessita de um aplicativo desenvolvido em Java chamado Evo-SDK. Segundo seus criadores, E-Sec Segurança Digital (2015), ele é um kit de desenvolvimento de certificação digital. Ele integra, a certificação digital com aplicações já existentes ou em fase de desenvolvimento.

Esse aplicativo é responsável pela criptografia e integração dos certificados digitais e leitores biométricos com o sistema e-CNH sem ele não seria possível realizar a alimentação do sistema.

Para realizar todos os processos primordiais do negócio são utilizados alguns sistemas digitais que auxiliam e organizam todo o fluxo de dados na empresa.

Quatro dos cinco sistemas são contratados por empresas especializadas no ramo de desenvolvimento de *software* e pagos mensalmente com uma taxa fixa. Um dos sistemas, tem adesão gratuita, porém cobra-se por serviços realizados pelos CFC's credenciados, sendo ele o e-CNHsp.

Cada um dos sistemas contratados tem sua particularidade, o sistema CFC-A é responsável pelo agendamento e controle das turmas matriculadas nas aulas teóricas e pelo envio dessas informações para o e-CNHsp via integração, ele é instalado localmente no servidor da Matriz. O sistema CFC-B também é instalado localmente no servidor da Matriz e é responsável pelo: cadastramento dos alunos, agendamento de aulas práticas, controle do fluxo de caixa, orçamentos, emissões de relatórios e contratos. O Procondutor é um sistema online, responsável somente pela reciclagem das CNHs que estouraram a pontuação e pela renovação das CNHs que estão em mau estado, funcionando como um CFC teórico a distância. Por fim se tem um sistema online de emissão e gerenciamento de boletos de cobrança, comumente chamado de "Making" pelos colaboradores. Ele tem a função de gerar boletos de cobrança junto à uma instituição financeira e consulta-los checando se foram pagos ou não.

Para comportar os sistemas abordados acima, o CFC possui em cada unidade, uma infraestrutura de rede montada com todos os dispositivos necessários, de modo que sejam suficientes para o funcionamento, como exigido pelo DetranSP em sua portaria nº 101 (SÃO PAULO, 2016).

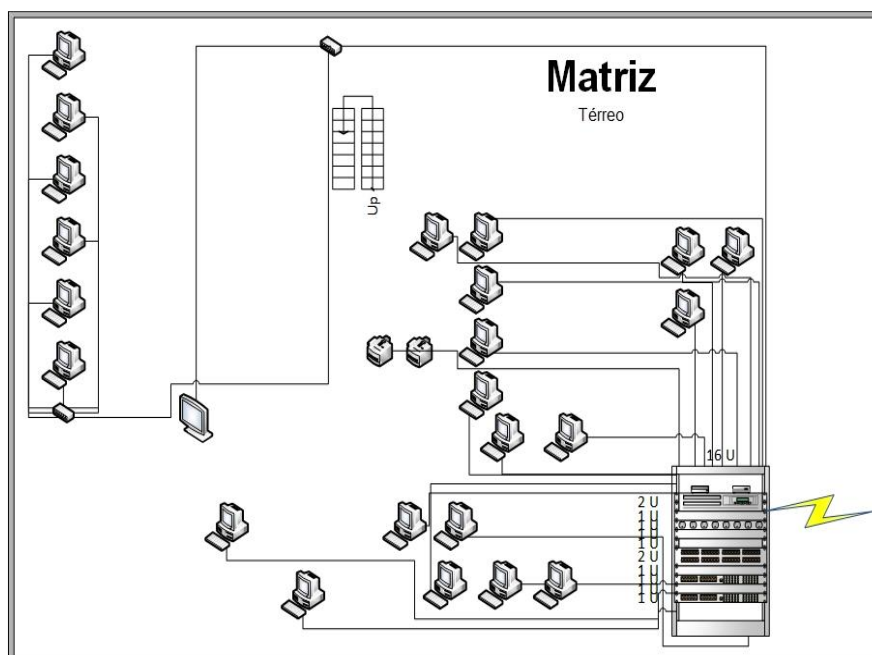
Abaixo está a relação de dispositivos do parque computacional de cada unidade, seguido pelas Figuras 3, 4, 5 e 6 com a distribuição desses equipamentos.

O parque de dispositivos de rede físico da Matriz é composto por:

- 30 Computadores
- 1 Servidor Dell
- 1 DVR (Digital Vídeo Recorder)
- 2 Impressoras Laser
- 1 Impressoras Térmica Etiqueta
- 1 Impressora Térmica de Recibo
- 1 Roteador TP-Link (Wi-Fi interno)
- 2 Links (NET 10MB, VIVO 100MB)

- 1 *Access Point* HotSpot 300 (Wi-Fi Convidados)
- 1 Switch 24x portas
- 2 Switches 16x portas
- 5 Simuladores da empresa Pro Simulador
- 1 Switch Hub 8x portas
- 1 Switch Hub 4x portas

Figura 3 - Distribuição dos dispositivos de rede no térreo da matriz



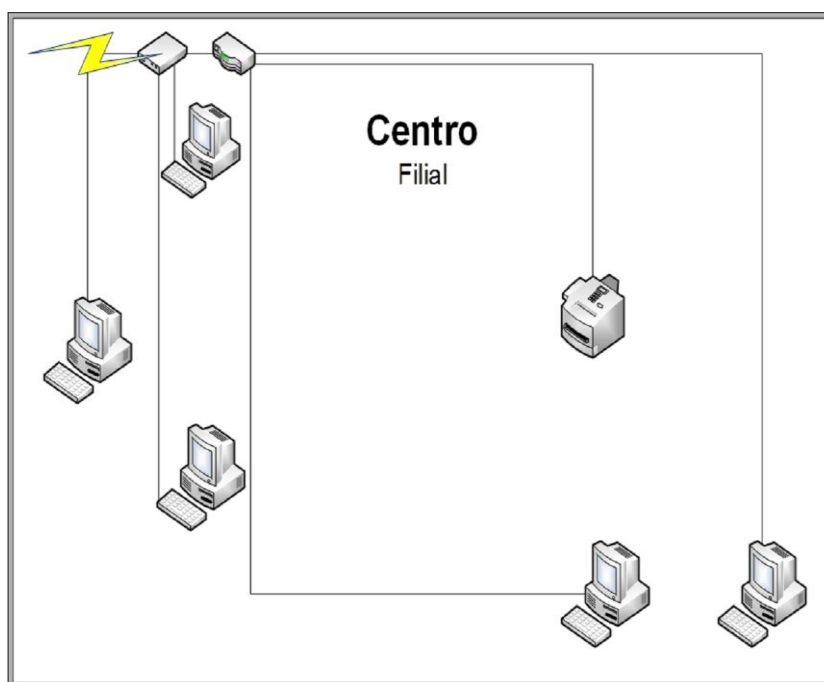
Fonte: Própria (2018)

Os dispositivos de rede nas filiais, são relativamente parecidos, tendo como único diferencial, o simulador na filial do Centro.

A filial do Centro possui:

- 4 Computadores
- 1 Impressora de rede
- 1 Simulador
- 1 Roteador Wi-Fi
- 1 Link (NET 30MB)

Figura 4 - Distribuição dos dispositivos de rede na filial do centro.



Fonte: Própria (2018)

A filial do Europa:

- 2 Computadores
- 1 Impressora de rede
- 1 Roteador Wi-Fi
- 1 Link (NET 30MB)

Figura 5- Distribuição dos dispositivos de rede na filial do Europa.

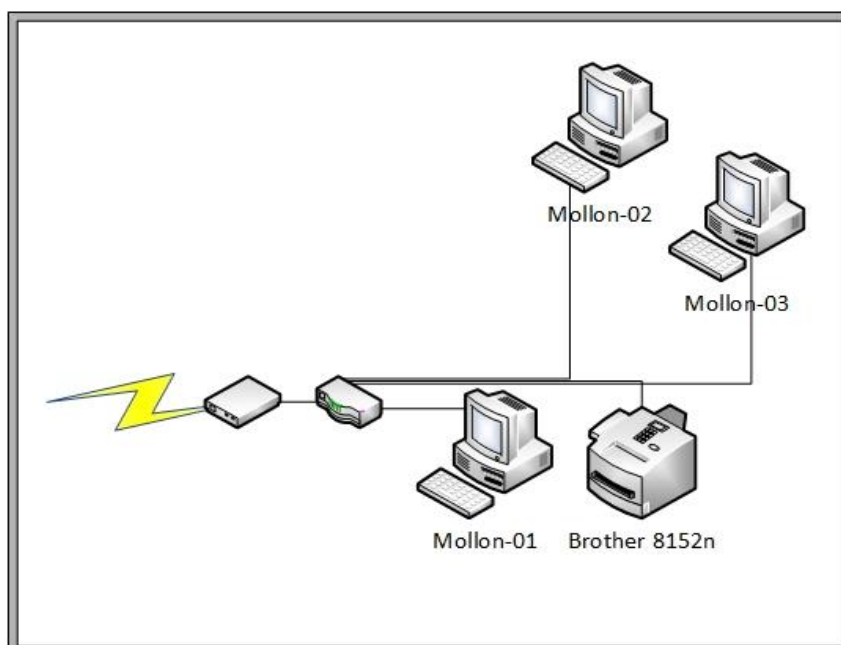


Fonte: Própria (2018)

E na filial do Mollon:

- 3 Computadores
- 1 Impressora de rede
- 1 Roteador Wi-Fi
- 1 Link (NET 30MB)

Figura 6- Distribuição dos dispositivos de rede na filial do Mollon.



Fonte: Própria (2018)

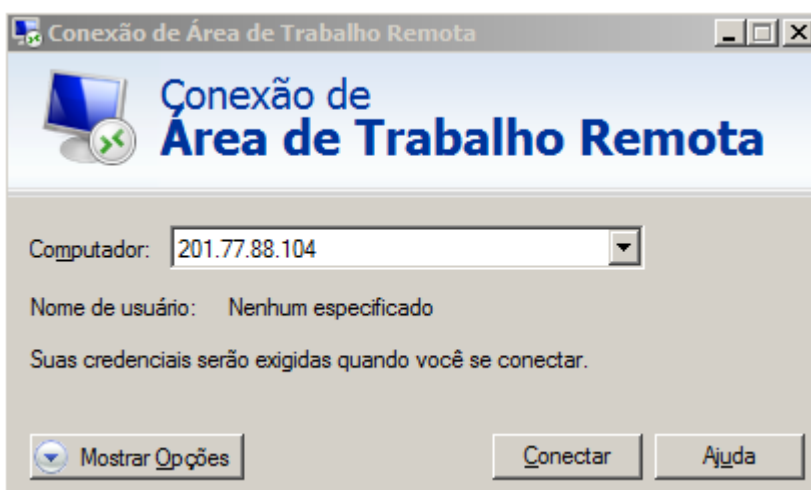
3.1 Ambiente antes das mudanças

A solução antiga para interligar todas unidades e centralizar o uso do sistema CFC-A e CFC-B era feita através do RDS (Remote Desktop Service) do Windows Server 2003. Ele era configurado no servidor da Matriz e aceitava a quantidade de conexões remotas, suficientes para atender as filiais e os próprios usuários da Matriz.

No roteador da Matriz era configurado um redirecionamento, para que todas as requisições feitas por qualquer endereço IP na porta 3389 seriam redirecionadas para o endereço IP do servidor na porta 3389, tornando-o vulnerável a possíveis ataques de quebra de senha e invasão, ocasionando um sério problema de segurança.

O acesso feito pelos usuários era realizado no próprio assistente de conexão remota do Windows, onde era configurado o IP remoto da Matriz e os acessos eram redirecionados para o servidor, exemplo na Figura 7.

Figura 7 - Exemplo conexão do usuário



Fonte: Próprio autor.

Quando havia alteração no endereço IP da Matriz, era necessário que todas as filiais alterassem o número de IP manualmente no assistente de conexão remota, causando transtornos e possíveis erros.

O Windows Server 2003 estava desatualizado e não havia organização de usuários, todos eles eram cadastrados como usuários locais no servidor, qualquer alteração de usuário necessária devia ser feita uma por uma, ocasionando retrabalho e aumentando as chances dos erros.

As pastas de trabalho também estavam localizadas no servidor, o mapeamento dessas pastas era realizado a mão, em cada estação de trabalho que necessitasse do seu uso, não havia controle de acesso aos arquivos, todos podiam acessar os arquivos sem exceções. Dessa maneira sempre ocorria perda de dados e muito retrabalho em uma eventual mudança de senha de rede.

Os computadores de trabalho não eram atualizados com frequência, havia muitos softwares dispensáveis e falta de padrão na configuração de cada um deles. O sistema operacional utilizado nos computadores era o Windows 7, mas não havia um padrão de versões, variando entre Enterprise, Professional e Ultimate.

Todos os usuários locais eram administradores e estavam frequentemente contaminados, principalmente pelo famoso vírus *Ransomware*¹, que trazia consigo diversos problemas ao responsável de TI. Nos computadores continham também, programas não autorizados, instalados pelos usuários, ocasionando diversos problemas e dores de cabeça ao suporte de TI.

Não havia política de senhas, todos os usuários colocavam sua senha de acordo com seu gosto, sem seguir nenhum parâmetro de segurança. Isso facilitava ainda mais as contaminações pelo vírus *Ransomware*.

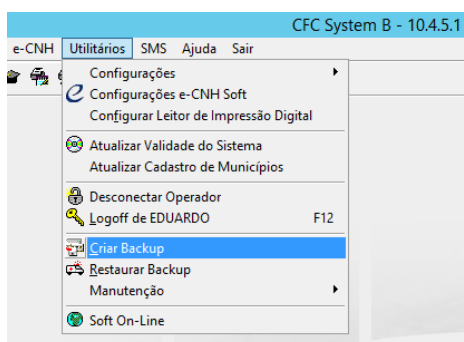
Devido a quantidade de ocorrências relacionadas ao vírus *Ransomware*, os colaboradores foram conscientizados para que tomassem alguns cuidados ao navegar na internet ou atualizar/abrir algum programa suspeito. Dessa forma, houve uma queda na quantidade de incidentes relacionados a esse vírus, mas ainda sim acontecia eventualmente.

A rotina de *backup* encontrada era realizada manualmente. Todos os dias as 17:30hs um alerta era enviado pelo responsável de TI a todos os colaboradores para que se desconectassem dos sistemas System CFC-A e System CFC-B para realizar

¹ “Ransomware é um malware de computador que restringe o acesso — ou até mesmo impede que você use seu computador — ou criptografa seus arquivos. Em seguida, ele tenta forçá-lo a pagar em dinheiro (um resgate) para recuperar o acesso aos arquivos” (MICROSOFT, 2018)

o *backup* de cada um. O responsável executava o gerenciador de tarefas do servidor e checava se havia alguma aplicação relacionada aos sistemas ainda em execução, se houvesse, à finalizaria. A partir da verificação o responsável acessava o assistente de *backup* do próprio sistema e fazia o *backup*, como se pode ver na Figura 8:

Figura 8 - Assistente de criação de backup System CFC-B



Fonte: Próprio autor.

O *backup* era salvo dentro do próprio servidor em uma pasta específica. Ao final da semana uma cópia de todos os *backups* era realizada para um disco rígido externo. O disco era conectado sempre que necessário. O *backup* das pastas de trabalho era realizado no mesmo período das 17:30hs, o responsável copiava manualmente para a pasta de *backups* e ao final da semana para o disco rígido externo. Ao final do mês o *backup* do mês anterior era excluído da pasta do servidor e se mantinha por três meses no disco externo. Não havia *backup* do sistema operacional, caso houvesse alguma falha no servidor, os sistemas e pastas de trabalho ficariam offline até que se reestabelece.

Os pontos de rede não eram identificados nem organizados, na ocorrência de algum eventual problema havia se perda de tempo para identificar e resolver a situação. Não havia um inventário atualizado do parque computacional, isso dificultava bastante o controle dos computadores, acessórios e insumos de informática. Devido a isso não havia um histórico de manutenção ou troca dos dispositivos. As manutenções só eram realizadas de forma corretiva, pois não havia dados registrados para manutenção preventiva ou preditiva.

Em resumo a rede do CFC Brasil funcionava mas não havia um gerenciamento efetivo da área de TI, havia se muito retrabalho e surpresas. Os

termos disponibilidade, integridade e confidencialidade não eram nem de longe atendidos e nem seriam resolvidos tão rapidamente.

3.2 Ambiente depois das mudanças

3.2.1 Active Directory

De início, foi alterado o sistema operacional do servidor mudando do Windows Server 2003 para o Windows Server 2013, que já não havia mais atualizações de segurança e a Microsoft já havia deixado de prestar suporte.

Em conjunto com o Windows Server 2013 foi implementado o serviço de domínio AD (*Active Directory*), que segundo a Microsoft (2017) presta serviços de domínio fornecendo os métodos para armazenar dados de diretório e tornar esses dados disponíveis para administradores e usuários de rede.

No modelo antigo, os usuários da conexão remota eram criados diretamente no servidor, dificultando muito o controle de cada um e gerando muito retrabalho, ou seja, quando havia a necessidade de alterar alguma permissão para determinado grupo de usuários se fazia necessário acessar cada membro do grupo e alterá-los individualmente.

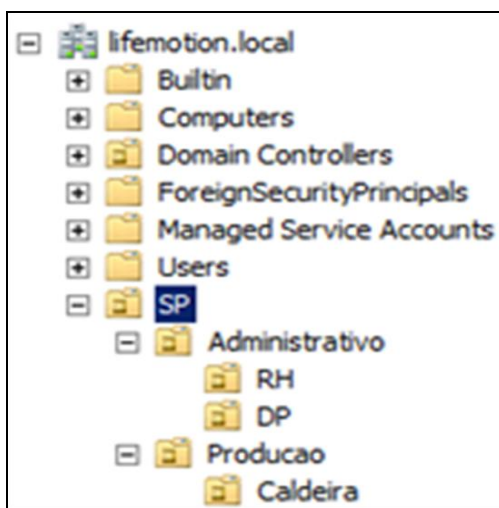
Era preciso que os colaboradores também tivessem acesso aos computadores locais, necessitando de mais um usuário pra isso. No modelo antigo os usuários eram administradores dos próprios computadores e por esse fato se tornavam suscetíveis a infecção por vírus, e causava diversos problemas na rede interna.

Para solucionar esse problema se pôs necessário o uso do AD. Ele é uma ferramenta muito extensa, podendo ser usada a níveis avançados ou não. Se tratando do CFC Brasil, somente algumas de suas funcionalidades foram utilizadas.

O AD foi instalado a partir do assistente do próprio Windows e configurado com as informações particulares da empresa. Foram criadas OUs (*Organizational Unit*) para organizar os usuários, segmentando e atrelando cada usuário ao seu

respectivo setor. A Figura 9, mostra a divisão dos setores por localidades e departamento, melhorando muito a organização dos objetos da rede:

Figura 9 - Exemplo organização por setores



Fonte: Microsoft (2015)

Os grupos/usuários criados através do AD auxiliaram nas permissões de acesso aos arquivos mapeados na rede. As permissões foram configuradas para distinguir o acesso de cada membro/grupo, aos arquivos da rede, solucionando o problema de acesso indevido a informações que não faziam parte de sua alçada.

Foram criadas também, algumas GPOs² (*Group Policy Object*) para controlar cada grupo de usuários da rede. As GPOs criadas tratavam de bloquear o acesso às funcionalidade técnicas do sistema, como: instalação ou alteração de programas/sistema, também auxiliava no mapeamento de pastas de trabalho e na política de senha utilizada por cada usuário.

Nas Figuras 10 e 11, pode se ver o exemplo da configuração de uma das GPOs do CFC Brasil. A primeira figura, representa as políticas aplicadas aos perfis de usuários, já a segunda representa as políticas aplicadas aos computadores que serão usados por algum usuário que fizer parte dessa GPO.

² A Group Policy (GPO), é capaz de mudar configurações, restringir ações ou até mesmo distribuir aplicações em seu ambiente de rede (BRANDÃO, 2018)

Figura 10 - Políticas para os perfis de usuários

User Configuration (Enabled)		
Policies		
Administrative Templates		
Policy definitions (ADMX files) retrieved from the local computer.		
Control Panel		
Policy	Setting	
Prohibit access to Control Panel and PC settings	Enabled	
Control Panel/Add or Remove Programs		
Policy	Setting	
Remove Add or Remove Programs	Enabled	
Desktop/Desktop		
Policy	Setting	
Desktop Wallpaper	Enabled	
Wallpaper Name: Example: Using a local path: C:\windows\web\wallpaper\home.jpg Example: Using a UNC path: \\Server\Share\Corp.jpg Wallpaper Style:		
Policy	Setting	
Prohibit deleting items	Enabled	
System		
Policy	Setting	
Prevent access to registry editing tools	Enabled	
<input type="checkbox"/> Disable regedit from running silently?		

Fonte: Próprio autor

Figura 11 - Políticas para computadores

Computer Configuration (Enabled)		
Policies		
Administrative Templates		
Policy definitions (ADMX files) retrieved from the local computer.		
Control Panel/User Accounts		
Policy	Setting	
Apply the default account picture to all users	Enabled	
System/User Profiles		
Policy	Setting	
Delete user profiles older than a specified number of days on system restart	Enabled	
<input type="checkbox"/> Delete user profiles older than (days)		
Policy	Setting	
Only allow local user profiles	Enabled	

Fonte: Próprio autor

O mapeamento das pastas foi configurado para ser executado sempre que o usuário fizer *logon*, assegurando sempre a disponibilidade dos arquivos. A política de senhas foi configurada para que atendesse somente à alguns parâmetros de complexidade, buscando não prejudicar os colaboradores mais velhos e com maior

dificuldade em memorizar as senhas, mas ainda assim, aumentando o nível de segurança. A nova política exige no mínimo:

- Seis caracteres.
- Uma letra maiúscula.
- Um número.

Com a introdução do AD dentro da empresa, foi possível alcançar maior organização e controle dos usuários, além dele proporcionar usuários que podem ser utilizados nos computadores locais, bastando inseri-los no domínio.

Para inserir os computadores no domínio foi necessário alterar o grupo de trabalho de cada computador para o domínio do CFC Brasil, assim cada sistema operacional seria apto à utilizar os usuários criados no AD e serem tratados pelas GPOs. Todos os usuários passaram a utilizar o mesmo usuário para realizar o *logon* nos computadores locais e no servidor remoto. O acesso como administrador local foi bloqueado e inibido através do uso de senha para autenticação, que fica em porte da TI.

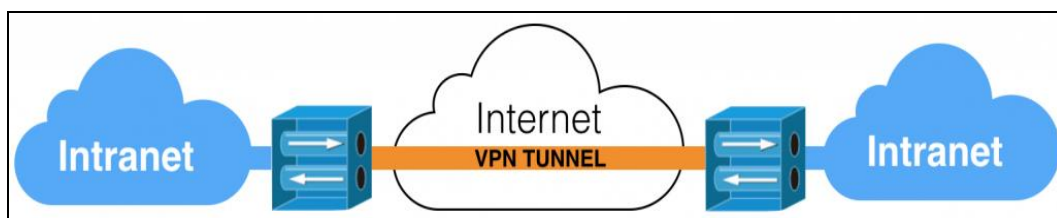
Com as GPOs surtindo efeito no ambiente local, solucionou-se boa parte dos problemas relacionados a instalação de programas e/ou infecções por vírus através de programas maliciosos.

3.2.2 VPN

A solução antiga para interligar as unidades era realizada via redirecionamento de portas no roteador, permitindo o acesso de qualquer endereço IP externo a rede da Matriz. A rede ficava muito exposta a tentativas de invasão, se por ventura realizassem uma varredura na rede encontrariam a porta 3389 aberta e as tentativas de força bruta poderiam ser iniciadas. Para evitar essa situação foi implementado uma VPN (*Virtual Private Network*) no servidor, seu acrônimo em português significa “Rede Virtual Privada” se tornando bastante sugestivo ao que representa.

O principal objetivo da VPN é criar uma rede em que somente usuários credenciados possam ter acesso de forma segura. Os dados são criptografados e enviados por um túnel de ponto a ponto, como na Figura 12:

Figura 12 – Conexão VPN



Fonte: GRIDELLI (2017)

No caso do CFC Brasil, se optou por usar o *software* livre OpenVPN. Segundo o *website* OpenVPN (2018), ele foi criado por James Yonan, com o objetivo de ser um software gratuito, rápido e que trabalhasse sobre o protocolo TCP/IP e UDP. Além de ser gratuito é muito seguro e recomendado por diversos especialistas da área de SI (Segurança da Informação), conforme encontrado no próprio site.

No servidor foi instalado o modo *server*, que é responsável por criar e autenticar as credenciais dos clientes e, também parametrizar as regras de conexão. O executável de instalação para Windows foi disponibilizado no próprio *website* do OpenVPN. Ele foi instalado e configurado com alguns parâmetros para o funcionamento e distribuição dos endereços IP na rede privada.

Na Figura 13 pode se observar um exemplo de configuração do servidor VPN.

Figura 13 - Exemplo do arquivo de configuração

```

1 local 0.0.0.0
2 port 29000
3 proto udp
4 dev tun
5
6 ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
7 cert "C:\\Program Files\\OpenVPN\\config\\server.crt"
8 key "C:\\Program Files\\OpenVPN\\config\\server.key"
9 dh "C:\\Program Files\\OpenVPN\\config\\dh2048.pem"
10
11 server 10.26.0.0 255.255.255.0
12 push "dhcp-option DNS 10.26.0.1"
13 push "dhcp-option WINS 10.26.0.1"
14
15 ifconfig-pool-persist ipp.txt
16 keepalive 5 60
17
18 cipher AES-256-CBC
19
20 comp-lzo
21 client-to-client
22 max-clients 50
23
24 persist-key
25 persist-tun
26
27 status ../log//openvpn-status.log
28
29 verb 3

```

Fonte: Próprio autor

Cada linha da Figura 13, representa um tipo de configuração para o servidor VPN:

- A linha um, representa o endereço IP em que o servidor está escutando as conexão. Por estar configurado 0.0.0.0, quer dizer que o servidor poderá receber conexões de qualquer endereço IP.
- A linha dois, a porta em que o servidor estará escutando as requisições.
- A linha três, o protocolo utilizado na conexão que no caso é o UDP³.
- A linha quatro, o dispositivo que será criado para a rede VPN.
- As linhas cinco, seis e sete, são os locais onde serão encontrados os certificados, chaves e arquivos de configuração.
- A linha oito, os IP que serão atribuídos aos clientes.

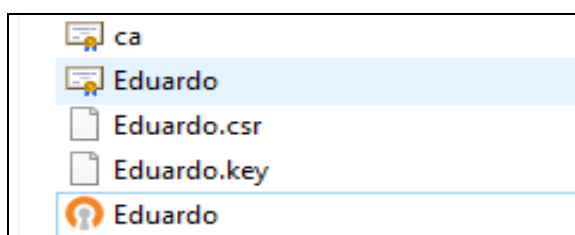
³ É um protocolo da camada de transporte que utiliza o mínimo de recursos possíveis para o comutação do pacote (RFC 768, 1980).

- As linhas nove e dez, forçam os clientes a pegarem os endereços de DNS e WINS que estão ali configurados.
- A linha onze, mantém em um arquivo de texto com a relação entre endereço e cliente para futuras conexões.
- A linha doze, monitora a conexão entre cliente e servidor. O primeiro valor colocado a frente representa o tempo de *ping* entre a conexão e o segundo valor representa o tempo para a reconexão.
- A linha treze, o tipo de criptografia usada.
- A linha quatorze, habilita a compressão de dados na VPN.
- A linha quinze, permite a comunicação entre clientes da VPN.
- A linha dezesseis, a quantidade de cliente simultaneamente conectados.
- As linhas dezessete e dezoito, garantem a permanência da interface TUN e da chave em uma eventual reinicialização da VPN.
- A linha dezenove, é o local onde serão salvos os logs da VPN.
- A linha vinte, é o nível dos erros que serão salvos em log, variando de 0-11, onde 11 representa qualquer tipo de erro e 0 somente erros fatais.

No servidor foram criadas credencias para todos os computadores das filiais, garantindo que somente os computadores certificados tivessem acesso ao servidor remotamente. Essa implementação solucionou o problema de exposição a ataques de força bruta e garantiu sigilo nas informações trafegadas entre as unidades.

Nos computadores das filiais se fez necessário instalar o OpenVPN em modo *client*, responsável por se conectar ao servidor da Matriz remotamente. Cada computador recebeu dois certificados, um arquivo de configuração, uma assinatura do certificado e uma chave, criados pelo servidor, como ilustra a Figura 14:

Figura 14 - Arquivos de Configuração cliente



Fonte: Próprio autor.

No arquivo de configuração do cliente foi inserido alguns parâmetros para estabelecer a conexão com o servidor. Na Figura 15, pode se ver um exemplo do arquivo:

Figura 15 - Arquivo de configuração do cliente

```

1 client
2 dev tun
3 proto udp
4 remote cfcbrasil.sytes.net 29000
5 resolv-retry infinite
6 nobind
7 persist-key
8 persist-tun
9 push "dhcp-option DNS 10.26.0.1"
10 ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
11 cert "C:\\Program Files\\OpenVPN\\config\\Eduardo.crt"
12 key "C:\\Program Files\\OpenVPN\\config\\Eduardo.key"
13 remote-cert-tls server
14 cipher AES-256-CBC
15 comp-lzo
16 verb 3

```

Fonte: Próprio autor

Cada linha representa um tipo de configuração que será executada para estabelecer a conexão com servidor. A lista abaixo relaciona a descrição da cada linha:

- A linha um, representa a identificação do computador como cliente.
- A linha dois, especifica o dispositivo que será criado para se conectar ao túnel VPN.
- A linha três, o protocolo que será utilizado na conexão.
- A linha quatro, o endereço remoto do servidor VPN
- A linha cinco, se o cliente restabelecerá conexão com o servidor. Variando os valores booleanos 0 e 1 para sim ou não ou, infinito para tentativas infinitas de conexões.
- A linha seis, não especifica a porta da conexão com o cliente.
- A linha sete, que a chave deve persistir em caso de perda de conexão.

- A linha oito, que o dispositivo tun criado deve permanecer na perde da conexão.
- A linha nove, que o cliente deve pegar o endereço de DNS ali descrito.
- A linha dez, onze e doze, são os caminhos lógicos que se localizam o certificado autoritário, o certificado pessoal e a chave.
- A linha treze, para permitir o estabelecimento da conexão TLS com o servidor remoto.
- A linha quatorze, a criptografia utilizada na conexão.
- A linha quinze, habilita a compressão de dados na VPN
- A linha dezesseis, é o nível dos erros que serão salvos em log, variando de 0-11, onde 11 representa qualquer tipo de erro e 0 somente erros fatais.

Conforme exposto nas configurações, tanto do cliente quanto do servidor, foram realizadas algumas alterações no padrão da configuração da VPN, como: mudança da porta padrão, utilização somente do protocolo UDP, utilização de criptografia 256 bits, criação de um DDNS⁴ (Dynamic Domain Name Server) para facilitar nas eventuais mudanças de IP, mudança no endereçamentos IP da VPN e, por fim, a não atribuição de um *gateway*⁵ na rede, fazendo com que os clientes usassem o gateway do próprio roteador para navegar na internet.

O problema relacionado a eventual troca de endereço IP do assistente de conexão remota, foi solucionado. A VPN faz com que o servidor possua um endereço IP privado e fixo, podendo ser atribuído aos assistentes de conexão sem que o usuário precise ficar alterando. Isso garante menos erros e maior disponibilidade.

⁴ DDNS transforma um endereço IP válido em um nome fixo na internet, ex.: exemplo.ddns.net. Ele fica responsável por verificar e atualizar em tempo real qualquer mudança no endereço IP e redirecionar para o nome criado.

⁵ É o equipamento que funciona como porta de saída para rede local. Funcionando como um intermediário entre a internet e a LAN.

3.2.3 Inventário e Organização

Os computadores do CFC Brasil, não estavam com o sistema operacional padronizado e não havia organização nominal dos mesmos. Os nomes eram inseridos de acordo com o nome do usuário criado na hora da instalação do Windows, prejudicando muito o levantamento de informações e de localização do seu posicionamento na rede. Com os sistemas operacionais sem padrão, ficava mais difícil elaborar diagnósticos e dar manutenções, pois os erros variavam de versões para versões além de terem algumas diferenças operacionais.

Um trabalho gradual foi feito na rede do CFC Brasil para regularizar o problema de organização. Todos os computadores foram modificados de forma geral, alguns mais radicalmente que os outros. Nos casos mais radicais foi necessário a reinstalação do sistema operacional e dos programas utilitários. Nos casos mais simples, somente a instalação ou desinstalação de programas que não atendesse o padrão novo proposto.

O padrão proposto para cada computador foi relacionado na tabela abaixo:

Tabela 1 - Programas padrão dos computadores

Programa	Descrição
Windows 7 Professional	É um sistema operacional da família de sistemas do Windows.
Avast Antivirus Free Edition	É um software de proteção contra vírus maliciosos, contendo diversos módulos de proteção.
Java Runtime Environment	Programa que compatibiliza o funcionamento de sistemas web desenvolvidos em java com browser do cliente.
Adobe Reader	Leitor e modificador de PDFs.
Daemon Tools Lite	Utilizado para emulador o driver de CD/DVD, possibilitando a leitura de mídias digitais com formato ISO, MDX, MDS, entre outras.
Programa	Descrição
E-SDK	Applet utilizado para o funcionamento dos leitores biométricos e leitores de certificados digitais em conjunto com o sistema e-CNHsp
Pacote Microsoft Office 2010	Programa que contém ferramentas que auxiliam o set administrativo, como: criação de textos, planilhas, apresentações, gráficos, cronogramas e etc....

Safesign	É um gerenciador criptográfico necessário para interpretação dos certificados digitais com formatos de cartões A1, A2, A3...
SafeNet Authentication Tools	É um gerenciador criptográfico necessário para a interpretação de certificados digitais com formato de tokens Aladin.

Fonte: Próprio autor (2018)

As escolhas dos programas foram baseadas nas configurações físicas dos computadores, nas tarefas desempenhadas na empresa e nas licenças de uso. Todos os softwares escolhidos são gratuitos, com exceção do sistema operacional e do pacote Office.

A migração do sistema operacional e do pacote Office para programas gratuitos, não foi possível ser realizada, os usuários não se adequariam a tal mudança e causaria um grande problema na funcionalidade do CFC Brasil. Licenças para esses programas foram compradas e os computadores regularizados conforme o padrão proposto.

Em meio as mudanças e padronização de cada computador, os nomes de cada um foram alterados de acordo com a sua posição física, por exemplo: CA-01 (Computador Administração - 01), CIFC-01 (Computador Instrutores Filial Centro – 01). Etiquetas foram feitas e coladas em cada um, com sua identificação.

Para organizar todo o inventário de computadores e dispositivos do CFC Brasil, uma ferramenta de auxílio foi implementada, o GLPI⁶ (*Gestionnaire Libre de Parc Informatique*). Essa ferramenta auxilia o administrador da TI à organizar todo o parque computacional de forma geral.

Segundo o *website* GLPI Brasil (2018), a ferramenta “foi criada para facilitar a vida dos gestores de TI. Ela permite o gerenciamento dos mais diversos tipos de requisições, incidentes, projetos e ativos”. Sendo uma ferramenta muito completa e robusta.

Na empresa CFC Brasil, foi implementado somente duas partes da ferramenta: o controle de inventário e controle de chamados. A longo prazo, a empresa pretende implantar mais recursos disponíveis na ferramenta.

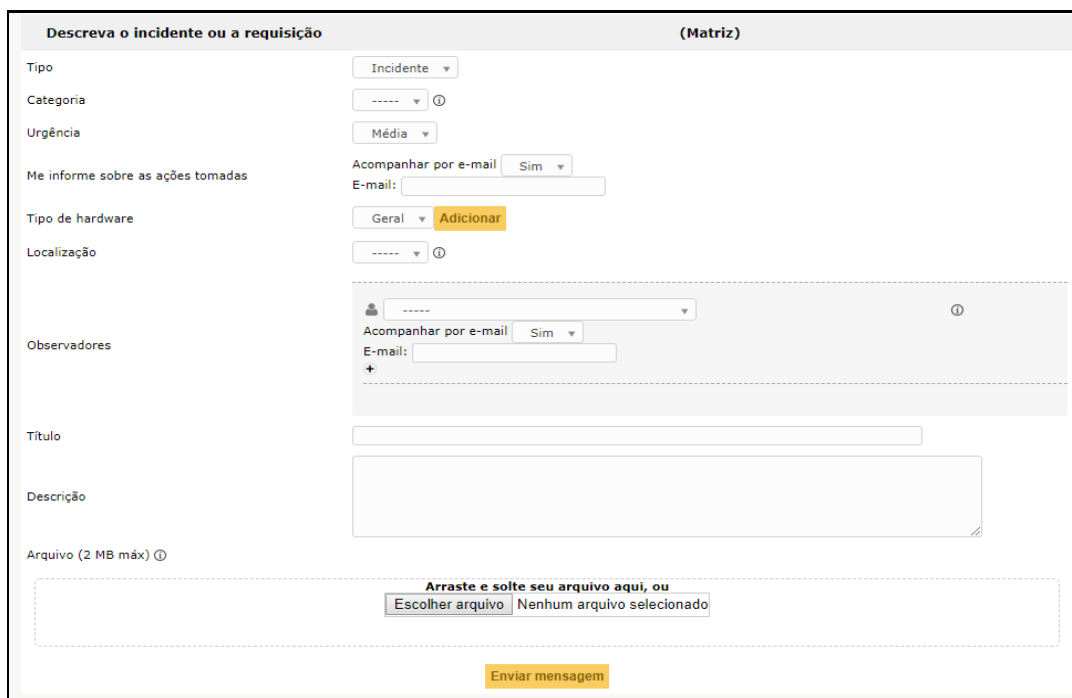
⁶ “O GLPI é uma aplicação de gestão de serviços e gerenciamento de ativos 100% web.” (GLPI BRASIL, 2018).

Todos os computadores padronizados foram cadastrados no inventário do GLPI, com seus respectivos hardwares e softwares. Os dispositivos de rede de todo o parque computacional, também foram cadastrados com suas devidas especificações.

Na ocorrência de um eventual problema em algum dos dispositivos do parque computacional, um chamado deve ser aberto e, as informações do acontecimento inseridas nos campos destinado. Ao final do chamado, a solução seria salva em um histórico facilitando futuras manutenções e diagnósticos.

A abertura de chamados ficou atrelada a todos os colaboradores da empresa, podendo realizar a abertura de chamados através do *login* no GLPI. Na tela de abertura de chamados, há campos suficientes para o usuário informar detalhadamente o incidente, além de poder acompanhar o estado do chamado criado. Um exemplo da tela de abertura de chamado vista pela interface de um usuário pode ser vista na Figura 16:

Figura 16 – Tela abertura de chamados no modo usuário



Descreva o incidente ou a requisição (Matriz)

Tipo:

Categoria: ⓘ

Urgência:

Me informe sobre as ações tomadas: Acompanhamento por e-mail:

E-mail:

Tipo de hardware:

Localização: ⓘ

Observadores: ⓘ

 Acompanhamento por e-mail:

 E-mail:

 +

Título:

Descrição:

Arquivo (2 MB máx) ⓘ

Fonte: Próprio autor.

A implantação do GLPI colaborou muito na organização do parque computacional, mas ainda havia problemas relacionados a identificação e organização dos pontos de rede. Os cabos de rede dentro do armário de telecomunicações estavam tão bagunçados que não era possível distinguir onde cada ponto estava conectado. Não havia *patch panels*⁷ instalados nem etiquetas de identificação nos cabos de rede, tornando qualquer mudança ou manutenção muito demorada e suscetível a erros.

Um trabalho árduo foi realizado no CFC Brasil para solução desse problema. Alguns equipamentos se fizeram necessários para realização do projeto, como: *patch panels*, *patch cords*⁸, rotulador, *punch down*⁹ e o testador de cabo de rede.

O início do projeto, foi marcado pela identificação dos cabos. Com o auxílio do rotulador e do testador de cabo de rede, um cabo era desconectado no *switch* e a busca pela outra ponta era iniciada, se um colaborador entrasse em contato avisando que estava sem internet facilitava o trabalho, se não o cabo era procurado um a um. Após encontrar as duas pontas, uma etiqueta era impressa e colada em

⁷ Pannel que organiza e conecta cabos de comunicação.

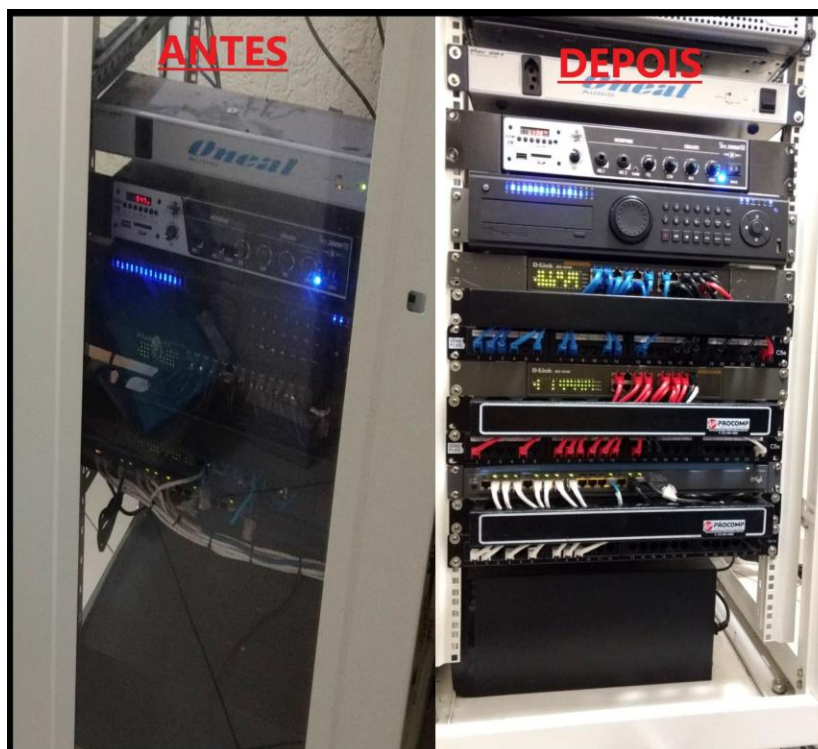
⁸ Cabo de rede para conexões curtas entre pontos.

⁹ Ferramenta utilizada para fixar os cabos no *patch panel*.

cada uma. As identificações dos cabos eram feitas de acordo com sua posição física, por exemplo: PA-01 (Ponto Administração – 01), PRC-01 (Ponto Recepção Centro -01).

Todos os cabos de rede foram refeitos e fixados no *patch panel* com o auxílio do *punch down*. Etiquetas também foram coladas nos espelinhos de cada porta do *patch panel*. Os *patch cords* foram utilizados para fazer a ponte de comunicação entre o *patch panel* e o switch e, receber etiquetas de identificação. A Figura 17, ilustra a organização do armário de telecomunicações antes e depois.

Figura 17 – Foto real do antes e depois da organização dos cabos



Fonte: Próprio autor

Todas as informações correspondentes a identificação da rede foram documentadas, facilitando futuras mudanças ou, até possíveis manutenções na rede.

3.2.4 Backup

Os *backups* no cenário anterior, eram realizados totalmente de forma manual, deixando toda responsabilidade sob um colaborador que, se caso viesse a faltar, no dia não seria realizado. Essa forma de *backup* trazia grandes riscos ao negócio, principalmente pela frequente infecção dos computadores pelo vírus *Ransovare*.

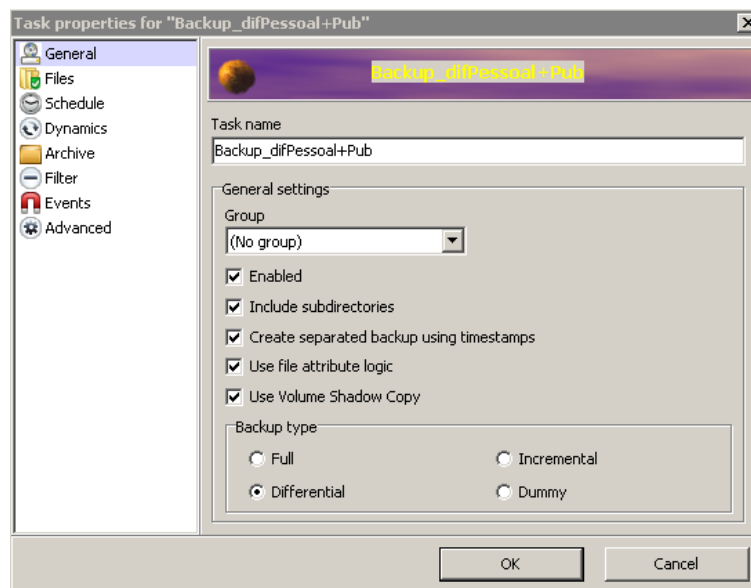
Uma ferramenta chamada Cobian Backup, que hoje está em sua décima primeira versão, foi utilizada para automatizar os *backups* feitos a mão. Segundo o *website* do Cobian (2009), a ferramenta foi criada para auxiliar um amigo que necessitava na época, copiar um arquivo que sumia todos os dias após exceder 1MB. A ferramenta funcionou tão bem que desenvolveu o interesse dos criadores em continuar a implementá-la. Chegando até os dias de hoje.

O Cobian foi escolhido pelo CFC Brasil, por ser uma ferramenta gratuita, simples e rápida, além de possuir diversos recursos que atendem muito bem ao que foi proposto.

A instalação do Cobian foi efetuada em um computador que estava parado, sem uso na rede. Por ele não ser uma aplicação pesada, não foi necessário dimensionar um servidor para isso, funcionando muito bem no computador. No *setup* de instalação do Cobian, é possível instalá-lo de duas formas, como: serviço ou como aplicação. No modelo de aplicação o Cobian só funcionará após um usuário iniciar uma sessão no sistema operacional. Já como serviço, o Cobian iniciará assim que o computador for ligado e carregar o sistema operacional, sem a necessidade do *logon* do usuário.

Ao criar-se uma primeira tarefa, ou *task*, como é chamado no próprio sistema, uma tela de configuração é exibida, mostrando as possíveis configurações que podem ser escolhidas.

Figura 18 – Propriedades das tarefas



Fonte: Próprio autor.

Na Figura 18, no canto superior esquerdo, encontra-se a lista de propriedades de uma tarefa. Cada item tem uma finalidade, de forma objetiva será explicado abaixo cada um dos itens:

General: É onde se insere o nome da tarefa e o tipo do *backup* que será efetuado. Também são realizadas configurações adicionais do *backup*, como: relacionamento de grupo, status da tarefa (ativado ou desativado), se incluirá subpastas ou não, se deve utilizar ou não ou arquivos de atributos lógicos dos usuários ou se deve utilizar *Shadow Copy*¹⁰.

Files: Todos os arquivos que serão copiados e o seus destinos são informados nessa opção. Suportando caminhos de rede, dispositivos de mídia físico e lógico.

Schedule: Nessa opção são informadas as datas, horas e os dias que serão executados os *backups*.

Dynamics: Qual o nível de prioridade de execução da tarefa e, se for *backup* diferencial ou incremental, quantas cópias completas devem ser mantidas.

¹⁰ “Trata-se de uma tecnologia Microsoft que funciona como uma interface de sistema (ou uma estrutura) que permite que ferramentas de terceiros executem backup e restauração centralizados” (HFTECNOLOGIA, 2018)

Archive: O tratamento do arquivo de *backup* é informado aqui. Qual a criptografia que será utilizado e o tipo de compressão.

Filter: Quais arquivos serão excluídos do *backup*. Por exemplo, a cópia não pode ter nenhum arquivo de mídia .mp3, é nessa opção que deve ser informado.

Events: Nessa opção configura-se os eventos precedentes e antecedentes a tarefa. Por exemplo, execução de scripts, programas ou, outras tarefas.

Advanced: Nas configurações avançadas, é informado qual usuário deve executar a tarefa. Também é informado configurações adicionais a nomenclatura do backup, como por exemplo, a inserção do nome do tipo do backup no nome do arquivo de *backup*.

Para garantir que a automatização dos *backups* fosse um sucesso, foi necessário o uso de três funcionalidades primordiais do Cobian, sendo elas: o *backup full*, *backup incremental* e *backup diferencial*.

Segundo o Red Hat (2005), os termos citados acima podem ser definidos de tal forma:

Backup full:

“Este tipo consiste no *backup* de todos os arquivos para a mídia de *backup*.”

Backup incremental:

Ao contrário dos backups completos, os backups incrementais primeiro verificam se o horário de alteração de um arquivo é mais recente que o horário de seu último backup. Se não for, o arquivo não foi modificado desde o último backup e pode ser ignorado desta vez. Por outro lado, se a data de modificação é mais recente que a data do último backup, o arquivo foi modificado e deve ter seu backup feito (RED HAT, 2005).

Backup Diferencial:

Backups diferenciais são similares aos backups incrementais pois ambos podem fazer backup somente de arquivos modificados. No entanto, os backups diferenciais são acumulativos — em outras palavras, no caso de um backup diferencial, uma vez que um arquivo foi modificado, este continua a ser incluso em todos os backups diferenciais (obviamente, até o próximo backup completo) (RED HAT, 2005).

O *backup full*, em vista aos demais, se mostrou mais seguro ao se realizar uma restauração rápida, em contrapartida, o salvamento dos dados é mais demorado se comparada aos outros métodos. Pensando nisso, ele foi utilizado para salvar o estado do sistema do servidor e os arquivos dos sistemas System CFC “A” e System CFC “B”. Por serem os protagonistas do funcionamento do negócio e, o tamanho total do *backup* não ser tão grande, não houve problema algum em adotar

esse método mais seguro. O dimensionamento do *backup* é feito pelo próprio Cobian, basta adicionar o caminho lógico do local que será salvo e ele se encarregará de contabilizar a quantidade de espaço necessário.

Nos demais *backups*, foi utilizado o incremental em conjunto com o diferencial, eles ficaram responsáveis somente em salvar os arquivos das pastas de trabalho do servidor. Uma coisa interessante encontrada nas opções de *backup* incremental e diferencial, é a possibilidade de programar uma data para o *backup full* dos arquivos que serão comparados ao longo do *backup* diferencial e incremental.

A política de *backup* que o CFC Brasil adotou, tem como objetivo garantir que, em uma eventual falha de sistema, perca-se somente um dia de informações e, que os *backups* antigos fossem mantidos pelo período de um ano. Para atender esse objetivo foi definido no Cobian, as seguintes regras:

- O *backup full* dos sistemas deve ocorrer todos os dias após as 23:00hs.
- O *backup* Incremental deve ocorrer todos os dias após as 23hs.
- O *backup* diferencial deve ocorrer no sábado após as 13hs.
- O *backup full* através do *backup* diferencial e incremental, deve ocorrer todo dia 1 do mês a partir das 23:00.
- Deve se manter os *backups full* durante 60 dias.

Esses horários e dias foram escolhidos de acordo com o funcionamento da empresa, sendo o último acesso às 22:30hs e aos sábados as 12:00hs.

Os locais destinados ao salvamento dos *backups* foram distribuídos pela rede e replicados em mais de um local. Essa distribuição ocorreu para garantir que o *backup* esteja sempre seguro em uma eventual necessidade. Em auxílio, uma dessas pastas destinadas ao *backup*, foi sincronizada com o aplicativo Google Backup e Sincronização. O aplicativo permite que os arquivos sejam salvos em nuvem e possa ser acessado de qualquer lugar, além de possuir versionamento de modificações, garantindo maior disponibilidade e integridade dos arquivos salvos (GOOGLE, 2018).

Aprimorando ainda mais as rotinas de *backup*, funcionalidades extras do Cobian foram utilizadas para aumentar o nível de segurança, organização e velocidade, na hora da sua execução, como:

-
- Compressão e criptografia dos arquivos de *backup*.
 - Execução de *script*¹¹ no início e final da rotina de *backup*.
 - Marcação de *timestamp*¹² em todos os *backups* feitos.
 - Não cópia de pastas vazias.

Os arquivos de *backup* foram comprimidos e criptografados, sendo necessário a inserção de senha para a descompressão. Isso evitava que em alguma eventualidade de vazamento, os arquivos contidos não pudessem ser utilizados.

Dois *scripts* foram criados para inserir e remover a letra da unidade removível que estaria conectada ao computador de *backup*, funcionando como um *mount* e *unmount* do Linux. Esses *scripts* foram configurados no próprio Cobian como tarefas prioritárias a serem executadas.

As *timestamps* inseridas nos nomes do *backup*, auxiliavam muito na organização dos *backups*. Se por ventura fosse necessário localizar algum arquivo de uma data específica, seria mais fácil de encontrar. As pastas vazias também atrapalhavam bastante à organização, podendo ser descartadas sem problemas.

¹¹ Conjunto de instruções executadas pelo computador para atingir determinada programação

¹² É uma marca temporal escrita por extenso, contendo data e hora.

4 RESULTADOS OBTIDOS

A implantação das mudanças causou ganhos reais, não só notado pelo setor de TI, mas por todos colaboradores do CFC Brasil. Apesar de todos ficarem um pouco confusos no início da implementação, ao decorrer foram se adequando e o trabalho começou a fluir melhor.

Pelo CFC Brasil ser uma estrutura que não havia quase que controle nenhum de TI, simples soluções como essas apresentadas ajudaram e muito a colaborar com o objetivo da empresa. Definidos em subcapítulos, os resultados tiveram muito mais prós do que contras, que podem ser acompanhados abaixo.

4.1 Interligação das unidades

Em relação ao primeiro problema descrito, sobre a interligação das filiais com a matriz. Houve ganhos notáveis de segurança e confidencialidade. A VPN proporcionou um ambiente limitado somente aos colaboradores certificados, inibindo tentativas de acesso externo por malfeitores. Além de criptografar os dados na conexão.

Em contrapartida, perdeu-se o dinamismo de acesso ao servidor, que podia ser feito de qualquer lugar a qualquer hora. Com o novo método, um certificado seria necessário para que o dispositivo se conectasse, impossibilitando o seu uso no momento. De certa forma, isso se tornou um benefício à organização, pois somente dispositivos autorizados pela TI efetuariam o acesso.

O problema de alteração do endereço IP no assistente de conexão remota, também foi solucionado. A VPN em conjunto com o DDNS permitiu que fosse efetuada uma configuração fixa, sem que os usuários precisassem ficar alterando o endereço quando eventualmente fosse mudado.

A utilização do protocolo UDP, tornou o transporte das informações um pouco inseguro, por não solicitar verificações nos pacotes enviados. Como a finalidade de seu uso era para realizar conexões remotas, entre cliente x servidor, essa possível

perda de pacotes não seria um estorvo, causando no máximo, alguns leves congelamentos.

O orçamento para implantação dessa solução de interligar as unidades, ficou restrito somente ao pagamento do colaborador de TI, pois não se fez necessário a compra de licenças ou equipamentos para elaboração do projeto.

No geral, essa mudança agregou bastante em relação ao cenário antigo, ganhos como:

- Segurança e privacidade no tráfego de informações
- Segurança ao estabelecer conexões entre as unidades
- Organização em relação aos locais que poderiam acessar remotamente o servidor.

Foram essenciais para aproximar ainda mais o CFC Brasil dos seus objetivos como empresa e, atingir um dos objetivos propostos nesse relatório.

4.2 Controle de Usuários

Com a implantação do Windows Server 2012 em conjunto com o AD, solucionou-se grande parte dos problemas relacionados a contaminação dos computadores pelo vírus *Ransomware* e a maioria das perdas de arquivos nas pastas mapeadas.

Com todos usuários sendo forçados a utilizarem sua conta de domínio, reguladas por GPOs, a instalação de programas e modificações de sistema, não foram mais possíveis, além de serem obrigados a inserir uma senha que atenda o mínimo de segurança parametrizada.

A parte negativa dessa mudança foi relacionada a cultura da empresa. Os usuários estavam mal acostumados, com senhas fáceis e muitas regalias de acesso, além de não precisarem digitar a famosa combinação de teclas “*Ctrl+Alt+Del*” no início de cada sessão. As reclamações eram constantes no começo, mas ao longo da implantação foram se esvaindo até acostumarem com o uso.

O custo de implantação dessa solução foi relativamente baixo. Foi necessário a compra de uma licença do Windows Server 2012 Standard, custando em média R\$ 1.700,00 e a compra de um servidor seminovo, custando em média R\$ 2.500,00. A

implantação do sistema foi efetuada pelo próprio colaborador de TI, barateando ainda mais a solução.

Mesmo com a difícil adaptação dos usuários no início, a solução trouxe ótimos resultados, como:

- Controle de acesso a arquivos.
- Controle de permissões de usuários centralizadas.
- Manutenção dos usuários de forma centralizada.
- Organização hierárquica dos setores.
- E maior segurança dos dados na rede local.

Todos esses pontos colaboraram para boa administração da rede, atingindo outro dos objetivos propostos.

4.3 Organização do parque computacional

A organização do parque computacional teve ótimos resultados, tanto para TI, quanto para os outros setores da empresa CFC Brasil. Em relação ao cenário antigo, que não era possível saber a posição dos equipamentos, o histórico de mudança de cada ativo ou, quantos chamados foram atendidos e o motivo deles, houve-se muitos benefícios, além de proporcionar transparência aos colaboradores sobre o trabalho da TI.

O custo para organizar todo o parque computacional também foi relativamente baixo, o sistema de gerenciamento GLPI é gratuito, competindo somente ao responsável de TI colocá-lo para funcionar. A organização física também foi executada pelo responsável de TI, gastando em média, com todos equipamentos para organização dos cabos, computadores e dispositivos de rede R\$ 1.500,00.

Toda essa mudança foi necessária, inclusive para apresentar o trabalho do setor de TI, que muitas vezes se encontra nas sombras da empresa.

Com os usuários podendo abrir chamados e registrar incidentes, a organização da TI ficou mais simples e completa, pois com as informações estando registradas futuras manutenções e resoluções de problemas ficariam mais fáceis.

Comparado ao cenário antigo, no qual não havia nenhuma organização, os resultados foram:

- Maior organização física dos equipamentos
- Aumento na qualidade dos atendimentos e manutenções
- Controle do fluxo de insumos de TI.
- Transparência da TI para os colaboradores.
- E transferência de conhecimento facilitada

Todos esses pontos colaboraram mais um pouco aos objetivos do CFC Brasil.

4.4 Automatização do Backup

Comparado ao modelo de *backup* antigo, realizado totalmente a mão, houve grandes melhorias, que serão descritas mais abaixo. Com a automatização, a responsabilidade de execução do *backup* foi totalmente transferida para máquina, ficando ao responsável de TI somente a responsabilidade de monitorar e, se necessário, modificar as configurações do programa.

Os dados foram salvos em horários estratégicos para que garantisse maior a quantidade de informações, caso acontecesse um eventual problema e necessitasse de recuperação.

Aos usuários, a mudança foi imperceptível a princípio. Ela foi notada após a necessidade de algum arquivo que foi excluído ou alterado. Normalmente esses arquivos do passado eram sempre perdidos, o usuário tinha que refazer todo o trabalho, em que muitas das vezes, não era possível ser reparado. Na nova solução era possível recuperar os dados alterados, aumentando a produtividade na empresa e evitando todo esse retrabalho.

Para a implantação dessa solução, não houve nenhum custo, a ferramenta é gratuita e foi configurada pelo próprio responsável da TI.

Ela garantiu maior disponibilidade, integridade e confidencialidade nos backups realizados, atendendo os três princípios da segurança da informação.

5 CONCLUSÃO E CONSIDERAÇÃO FINAL

Os cenários de antes e depois, ficaram totalmente distintos em seu funcionamento. Aos olhos dos usuários, não houveram tantas mudanças quanto para o setor de TI. O trabalho representou em sua maioria, a organização do ambiente TI perante aos processos de trabalho, em conjunto com medidas básicas de segurança da informação, que serão aperfeiçoadas constantemente ao longo do tempo.

O projeto de melhoria atendeu muito bem ao seu objetivo, iniciando a adesão dos princípios de segurança da informação no CFC Brasil. Ainda há diversas soluções a serem implantadas, fortalecendo ainda mais o que já foi construído e, aproximando a empresa de completar seus objetivos, missões e valores.

Ferramentas importantes como de monitoramento e filtro (*firewall*¹³ e *proxy*¹⁴), estão sendo estudadas para futuras implantações. Políticas de SI também serão estabelecidas de acordo com a cultura da empresa.

Os colaboradores do CFC Brasil, apesar de não terem se adequadado muito bem no início das mudanças, produziram muito mais, com menores quantidade de falhas. A proposta de um sistema de gestão mais inteligente e atual, também está nos planos da empresa, a ideia é que ele colabore ainda mais com a segurança da informação e usabilidade de seus processos.

Portando, este é um projeto a longo prazo que será sempre atualizado de acordo com as mudanças realizadas. Ele marcou o início de uma longa jornada de melhorias constantes, buscando se aproximar ao máximo do ideal da segurança da informação.

¹³ “Um Firewall é um sistema informático constituído por hardware e software específico cuja função é reforçar a segurança entre duas redes” (VENTURA; SOUSA; GOMES, 2001)

¹⁴ “Em linguagem simples, um Proxy não é mais que um intermediário que actua como cliente/servidor e que permite acesso a redes exteriores à nossa rede” (VENTURA; SOUSA; GOMES, 2001)

Referências

BENETTI, T. **Segurança da Informação – Confidencialidade, Integridade e Disponibilidade (CID)**. 2015. Disponível em:

<<https://www.professionaisti.com.br/2015/07/seguranca-da-informacao-confidencialidade-integridade-e-disponibilidade-cid/>>. Acesso em: 22 abr. 2018.

BRANDÃO, R. **Introdução a Group Policy (GPO)**. 2018. Disponível em: <[https://technet.microsoft.com/pt-br/library/cc668545\(d=printer\).aspx](https://technet.microsoft.com/pt-br/library/cc668545(d=printer).aspx)>. Acesso em: 17 nov. 2018.

CFCBRASIL. **Quem somos**. 2015. Disponível em: <<http://cfcbrasil.com.br/quem-somos/>>. Acesso em: 19 nov. 2018

CISCO. **Como as redes virtuais privadas trabalham**. 2008. Disponível em: <https://www.cisco.com/c/pt_br/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html>. Acesso em: 19 nov. 2018.

COBIAN, L. **Cobian Backup's evolution**. Disponível em: <<http://www.cobiansoft.com/cbevolution.htm>>. Acesso em: 19 nov. 2018.

DEBSOLUTIONSTI. **Conheça a ISO 27000 a família de normas que abordam a segurança da informação**. Disponível em: <<https://debsolutionsti.com/iso-27000/iso-27000/>>. Acesso em: 10 abr. 2018.

E-SEC SEGURANÇA DIGITAL. **Evo SDK**. 2015. Disponível em: <<http://www.esec.com.br/evo-sdk/>>. Acesso em: 05 abr. 2018.

GLPI BRASIL. **Conheça um pouco mais**. Disponível em: <<http://www.glpibrasil.com.br/por-que-se-registrar/>>. Acesso em: 18 nov. 2018.

GOOGLE. **Faça backup dos seus arquivos com segurança**. 2018. Disponível em: <https://www.google.com/intl/pt-BR_ALL/drive/download/backup-and-sync/>. Acesso em: 18 nov. 2018.

GRIDELLI, S. **Monitoring VPN connections**. 2017. Disponível em: <<https://netbeez.net/blog/monitoring-vpn-connections/>> Acesso em: 18 nov. 2018.

HFTECNOLOGIA. **O que é VSS?** 2018. Disponível em: <<https://hftecnologia.com.br/o-que-e-vss/>>. Acesso em: 18 nov. 2018.

MARINHO, R. **O que é Active Directory Topologia Física e Lógica: Parte 1**. Disponível em: <<https://social.technet.microsoft.com/wiki/pt-br/contents/articles/11423.o-que-e-active-directory-topologia-fisica-e-logica-parte-1/revision/2.aspx>>. Acesso em: 18 nov. 2018.

MICROSOFT. **Proteger seu computador contra ransomware**. 2018. Disponível em: <<https://support.microsoft.com/pt-br/help/4013550/windows-protect-your-pc-from-ransomware>>. Acesso em: 16 nov. 2018.

MICROSOFT. **Visão geral dos serviços de domínio do Active Directory**. 2017. Disponível em: <<https://docs.microsoft.com/pt-br/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>>. Acesso em: 17 nov. 2018.

NO-IP. **O que é DNS e DNS Dinâmico?** 2018. Disponível em: <<https://www.noip.com/pt-BR/what-is-dns>>. Acesso em: 19 nov. 2018.

OPENVPN. **Getting started**. Disponível em: <<https://openvpn.net/vpn-server-resources/getting-started/>>. Acesso em: 17 nov. 2018.

PRODESP. **Adesão ao e-CNH-sp**. Disponível em: <http://www.prodesp.sp.gov.br/e_cnh/comunicacao_adesao_ecnhsp_B.html>. Acesso em: 27 jan. 2018.

PRODESP. **Manual de Procedimentos para Utilização do e-CNHsp**. Disponível em: <http://tiraduidas.e-cnhsp.sp.gov.br/Manual%20CFC_AB_dez%202011.pdf>. Acesso em: 19 abr. 2018.

PRODESP. **O que é?** Disponível em: <http://tiraduidas.ecnhsp.sp.gov.br/oque_e.html>. Acesso em: 23 mar. 2018.

RED HAT. **Red Hat Enterprise Linux 4: Introdução à Administração de Sistemas**. [ebook]. Disponível em: <http://web.mit.edu/rhel-doc/4/RH-DOCS/pdf/rhel-isa-pt_br.pdf>. Acesso em: 19 Nov. 2018.

SÃO PAULO. Departamento Estadual de Trânsito. **Portaria DETRAN-SP nº 101, de 26 de fevereiro de 2016**.

SEBRAE, **Ponto de Partida para Início de Negócio**: autoescola (Centro de Formação de Condutores). 2007. Disponível em: <www.sebraemg.com.br>. Acesso em: 27 jan. 2018.

SEBRAE. **Como montar uma autoescola**. 2015. Disponível em: <<http://www.sebrae.com.br/sites/PortalSebrae/ideias/Como-montar-uma-auto-escola>>. Acesso em: 20 abr. 2018.

SÊMOLA, M. **Gestão da Segurança da Informação**. Rio de Janeiro: Elsevier, 2003.

VENTURA, C.; SOUSA, H.; GOMES, J. **Proxy, Firewall e Gateway: O que é proxy?**. 2001. Disponível em: <<https://paginas.fe.up.pt/~goii2000/M3/proxy.htm>>. Acesso em: 18 nov. 2018

VENTURA, C.; SOUSA, H.; GOMES, J. **Proxy, Firewall e Gateway: O que é firewall?**. 2001. Disponível em: <<https://paginas.fe.up.pt/~goii2000/M3/firewall.htm>>. Acesso em: 18 nov. 2018